Information Management

Accountability for Information Management: A Model

November 2004

Alberta
GOVERNMENT OF ALBERTA

Produced by:

Government and Program Support Services
Information Management Branch
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web sites:
www.im.gov.ab.ca
www.gov.ab.ca/foip
www.pipa.gov.ab.ca

© Government of Alberta

ISBN 0-7785-3115-5

Contents

1. Introduction 1

2. Accountability For Information Management 3

Program Executives and Managers

Ministry Employees

Information Management Director

3. Coordination and Integration 7

Information and Technology Strategic Coordination

Information and Technology Integration

4. Accountability in Practice: Roles and Responsibilities 10

Roles and Responsibilities

Roles and Responsibilities in Practice

5. Conclusion 17

1. Introduction

Information is a valuable asset for the Government of Alberta. To ensure this asset is managed to support government programs and services, Deputy Ministers adopted the Information Management Framework in 2003. A key principle of the framework is accountability – the need to identify clear roles and responsibilities for managing information assets within ministries.

Directive 3.2 of the Information Management Framework states:

> *"Ministries will develop accountability structures related to information management practices."*

Of course, how individual ministries go about implementing this directive will depend on a number of factors – its size, organizational structure, and existing accountability frameworks.

About this guide

This guide is intended for those individuals within ministries who have been charged with leading the implementation of the Government of Alberta Information Management Framework.

The guide presents a model accountability structure. **It is intended to be used as a starting point for the development and implementation of formal roles and responsibilities related to information management. As such, it is NOT prescriptive.** Rather, ministries will want to develop and implement an accountability structure that meets their particular business needs.

A good accountability structure will have three characteristics:

1. Clear accountability statements for the management of information assets within the ministry.

105-05401/

2. A mechanism for coordinating information management within the ministry and to ensure that information management is integrated with information and communications technology management and clearly supports knowledge management.

3. Clear identification and education around roles and responsibilities in specific business contexts.

Part 2 of the guide presents a model accountability framework. Then, in Part 3, models for coordination and integration are presented. Finally, in Part 4, roles and responsibilities are examined in the context of the life-cycle of information and illustrated in various business contexts.

2.
Accountability for Information Management

In today's business environment, everyone is a manager of information. Clearly articulating the accountability at all levels of the organization will support the appropriate management of information assets.

The Deputy Minister is ultimately accountable for the management of information in the custody or under the control of the ministry. This accountability is usually delegated to program managers and individual employees in the ministry. In addition, specific responsibility for providing leadership, expertise, and a focal point for managing information assets is often assigned to a specific function such as an Information Management Director.

This section lists a set of possible accountability statements for different levels and functions within the organization.

Program Executives and Managers

Program Executives and Managers are accountable, within their business area, for:

- identifying and defining information needed to meet short-term and long-term business objectives;
- ensuring the accuracy, completeness, and timeliness of information;
- ensuring practices for the proper collection, creation, storage, access, retention, and disposal of information are in place for employees and contractors and that these practices meet ministry policies and standards;
- ensuring the proper levels of security and privacy protection are applied to the information based on privacy impact assessments and threat/risk assessments and any relevant information sharing agreements;
- assessing the information management training needs for staff in the business area; and

- providing tools, technology and training to support their organization's management of information.

Ministry Employees

All ministry employees are accountable for:

- familiarizing themselves and complying with the information management policies, standards and practices;
- creating ministry documents in a timely manner that provide concise, accurate and complete evidence of their decisions, transactions and activities;
- identifying documents that warrant capture as official ministry records because of their business content;
- capturing the relevant contextual information and metadata describing electronic documents that are identified as official ministry records;
- ensuring only necessary records are created;
- ensuring transitory records created or received are disposed of regularly and in accordance with ministry standards;
- complying with all information security, confidentiality and privacy protection requirements of the ministry;
- ensuring official ministry records are only destroyed in accordance with authorized retention and disposition schedules;
- classifying, categorizing and storing information according to ministry guidelines for appropriate sharing, reuse and tracking; and
- identifying training and skills development needs in consultation with their manager or supervisor.

Information Management Director

As with other core assets – financial, human, technology – more and more organizations have developed a formal function to provide leadership, expertise, and a focal point for the management of information assets. This **function** is described here as the Information Management Director (IM Director).

The function of the IM Director is to ensure that information is managed as a corporate asset, that a strategic direction is set for the ministry with respect to information management and to establish consistent practices for information management. The IM Director provides leadership and support to business units and individuals responsible for information management on a day-to-day basis. Ultimately, the IM Director will supply three key benefits to a ministry:

- They will provide strategic direction regarding information management practices within the ministry.
- They will coordinate the implementation of effective and efficient information management practices within the ministry.
- They will provide specialized knowledge to support information management practices within the ministry.

The IM Director is accountable for:

- supporting business managers in identifying and meeting information management needs;
- developing information management plans for the ministry;
- leading and monitoring progress in implementing the government's Information Management Framework within the ministry;
- facilitating a coordinated approach to information management in the ministry to ensure all practitioner communities are working to achieve an overall strategic information direction of the ministry;
- developing ministry information management policies, standards and guidelines related to collection, creation, storage, access, retention, and disposal of information;
- helping business units define and understand their roles and responsibilities related to information management;
- providing advice to business managers across the ministry to create processes and procedures which will facilitate strong management of information assets;
- working with the Chief Information Officer (CIO) and information technology managers to plan and implement appropriate technology to effectively manage information assets;

- ensuring information planning is integrated into business planning, business continuity planning, accommodations planning and related initiatives such as knowledge management;
- working in conjunction with other ministries, through the cross-government Information Management Advisory Committee (IMAC), to ensure that the common standards for managing information which have been developed by IMAC (and supported by CIO Council and Administrative Services Council) are suitable and are being implemented within the ministry; and
- working with business units and other ministries to identify opportunities for information sharing, consolidation and coordination.

3.
Coordination and Integration

In reality, managing information assets needs to be coordinated between program managers, information management professionals and information technology professionals.

The Government of Alberta's Information Management Framework mandates that information management be coordinated to create a robust and sustainable information management regime.

Information and Technology Strategic Coordination

Many ministries have established coordinating bodies – a Ministry Information and Technology Strategy Coordination team (or sometimes called the Information Management Coordinating Committee). This team is made up of key IT managers, information management professionals (e.g. IM Directors, FOIP administrators, records managers, web site managers), and functional business unit managers (e.g. Branch or Division). The team is responsible for:

- interpreting the needs, wants, and desires of the member business units and translating those into priority IT/IM initiatives;
- setting the strategic direction for information management for the ministry;
- ensuring that IT/IM policies and investments are aligned with business priorities from across the ministry;
- ensuring that projects and initiatives are aligned to deliver, in a coordinated way, information and technology policies, procedures, and services;
- providing a forum to establish priorities for ministry IT/IM initiatives and investments;
- leveraging the best value from current information and technology investments; and
- ensuring there are appropriate linkages between information management and knowledge management activities.

Information and Technology Integration

The Chief Information Officer (CIO), the IM Director and the IT Director work together to manage both information and technology within the ministry. The roles of CIO, IT Director, and IM Director may be filled by a single individual in a small organization and by a number of people in a large organization.

Within the Government of Alberta, there are emerging models for coordinating information management accountability in various ministries. Figures 1 and 2 present two models currently established in some six ministries.

Figure 1
Model 1:
Ministry Information and Information Technology Functions

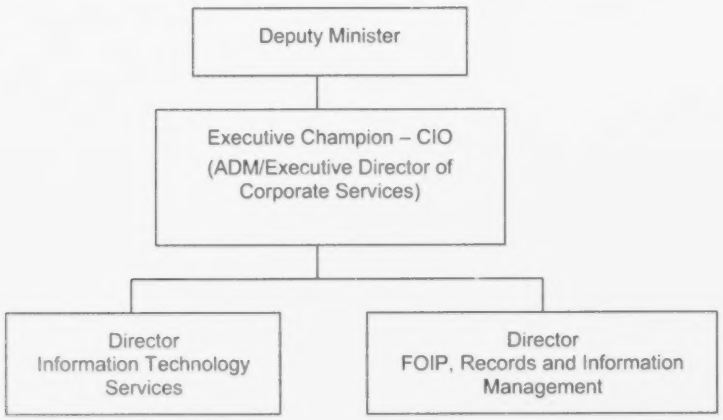
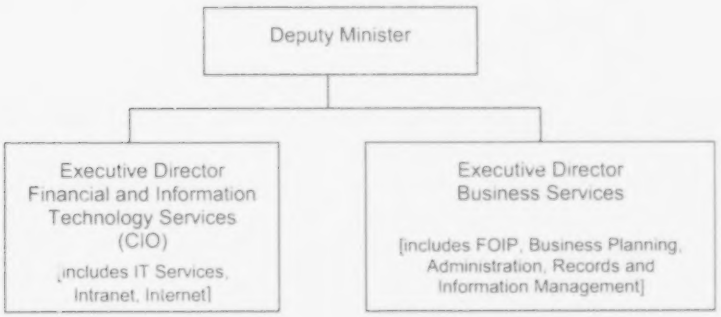


Figure 2:
Model 2:
Ministry Information and Information Technology Functions



4.
Accountability in Practice: Roles and Responsibilities

Any asset in an organization has people who **create** or **receive** the asset, who **use** the asset, and who **manage** the asset. In day-to-day business activities, a single individual will have multiple roles and responsibilities depending on their activities. As well, more than one person can be associated with specific roles and responsibilities.

Roles and Responsibilities

Various roles can be applied to the use and management of any given piece of information. These roles are:

- **Controllers**[1] are ultimately responsible for the information to support their business objectives. Controllers are often the business managers, although specific responsibilities of the controller might be assigned to work groups or to individuals.
- **Stewards** create, collect and receive information to support business activities. Stewards also update, edit, and ensure the accuracy of information and manage its use and disclosure. Finally, stewards ensure appropriate categorization of information to support sharing, future reference and reuse. Stewards are usually individual employees or work groups.
- **Administrators** design, implement and maintain the environment in which information is organized and stored. Examples of administrators are records management personnel, network administrators, Internet and intranet administrators, and library professionals.

[1] In some organizations, the controller is referred to as the information owner. The term owner has not been used here because information is not owned by individual employees – it is owned by the Government. It is a Crown asset.

- **Users** need information to make decisions or complete tasks. While users may be internal or external to the ministry (the public, clients and stakeholders), the focus in this document is on the roles and responsibilities of internal users.

Information Controllers

Controllers define information to meet business objectives.

Controllers are **responsible** for:

- identifying the needs of the information user and determining the information products that will meet those needs;
- ensuring the accuracy, completeness, and timeliness of information;
- ensuring legislative and policy requirements are followed regarding the proper collection, creation, access, use, security, disclosure, retention and disposal of the information;
- defining and ensuring the proper levels of security classification and privacy protection are applied to the information;
- selecting and managing the stewards of their business area's information;
- ensuring appropriate training is provided for new employees; and
- ensuring that information assets are appropriately managed when an employee leaves the business unit.

Information Stewards

Stewards support controllers in the collection, updating and management of information to support business objectives. Stewards can expect to know the requirements and expectations of information controllers.

Stewards are **responsible** for:

- creating, receiving, or collecting information to support the business;
- defining the context and applying metadata to the information when it is created;

- updating information accurately, completely and in a timely manner;
- classifying information security and protecting information from improper disclosure or unauthorized access; and
- assisting in any responsibilities of the controller that have been identified for the steward.

Information Administrators

Administrators advise and support stewards and controllers in managing information. Examples of administrators are records management personnel, network administrators, Internet and intranet administrators, and library professionals.

Administrators are **responsible** for:

- designing, implementing and maintaining the environment in which information is organized, stored and disseminated, including the setting of standards and practices;
- ensuring the availability of information for controllers, stewards, and users;
- providing advice to controllers and stewards on legislative and policy requirements for the collection, use and disclosure of information;
- administering proper security of the information in custody or control of the ministry.

Users

Users need information to make decisions or complete tasks. In the context of accountability for information management within ministries, the discussion of users focuses on internal users (i.e. government employees). This is not meant to ignore the vast amount of information that is designed for and disseminated to external users of government information (i.e. the public, clients and stakeholders). Rather, the focus is on internal users in establishing roles and responsibilities for information management within ministries.

Internal users should be able to expect:

- information is reliable – that it is sufficiently accurate, complete, and timely so that it may be used to make decisions or perform tasks;
- to access the information needed to perform their job; and
- to know who is the controller of the information.

Internal users are **responsible** for:

- using information which they are authorized to access; and
- protecting information from improper disclosure or unauthorized access.

Roles and Responsibilities in Practice

In practice, an individual may fulfill any or all of these information management roles from time to time, depending on the business context. This section provides illustrations of the roles and responsibilities in practice. The following contexts are illustrated:

- a committee or working group;
- creating and using day-to-day office documents;
- developing Internet content;
- managing information assets in a library or resource centre;
- developing a database application; and
- managing information through the application of electronic information management (EIM).

Here are some examples of how these roles may be fulfilled.

Example #1: Committee or Working Group

You've just formed an Information Management Coordinating Committee in your ministry. The committee will generate lots of information – both for itself as well as for employees in the ministry. The Chair of the committee, acting with the input and advice of the members will have the responsibility of **controller**, defining the

information needs of the committee. The committee will need to assign the role of **steward** for the information that is generated by the committee. The steward role may be played by the Chair of the committee, or it may be played by a Secretariat for the committee (e.g. the office of primary responsibility for the committee). The steward will create, collect, update and store, and manage information created by the committee. The **administrator** role will be shared by the system administrator (manages the network and servers on which the information resides), as well as other information management professionals (who manage the classification structure, and the retention and disposition standards for information in the ministry). In this case, depending on the type of information, the **user** may be committee members (e.g. agendas, minutes of meetings) or other employees (e.g. guidelines for information management).

Example #2: Day-to-Day Office Documents

You have created a spreadsheet for your own use. In this case, you will fulfill most of the roles identified above. You are likely the **user** (making decisions from the information), the **controller** (you define the information needed), and the **steward** (you create and update the information). In this case, the **administrator** role is shared by records management and information systems (they helped you define the folder and classification structure that helps you know how to name the spreadsheet and where to file the spreadsheet as well as maintain the servers on which the spreadsheet resides).

Example #3: Internet Content

Your program area has just created some new content for your ministry's web site. The **controller** of the information is the program manager (or delegated individual) that approves the content for dissemination. However, Communications also likely plays a controller role in terms of release of information to the public. The **steward** for the information may be the web development team or business author. The steward will be responsible for creating and updating the information. The **administrator** role would include whoever manages the site as a whole and the technical environment in which the content resides – as well as any others that may set standards for quality, including the look and feel or presentation of the information. Finally, as you developed the content, you identified the **users** of this information (likely the public or a group of clients or stakeholders).

Example #4: Library

In the context of a library or resource centre, the **controller** is the business manager or area that defines the need for information to be collected or disseminated. The **steward** role is played by the library staff in ordering, processing and managing the use of the resource materials (who may borrow and for how long). Library staff responsible for establishing and overseeing library management practices, including collections management, descriptions and classifications, and library systems fulfill the **administrator** function. Finally, the **user** may be anyone who has access to the library or resource centre.

Example #5: Database Application

Under legislation, your ministry is responsible for monitoring activities of businesses and organizations in a particular industry. Part of your mandate is to investigate complaints and issue orders related to infractions. The legislation also requires you to report on the level of compliance. To manage this information, you develop a case management system. The **controller** of the information is the business manager with the delegated ministerial responsibility for this business activity and how the information collected will be used. The controller function may also be delegated to a group of employees or to an individual employee. The **steward** of this information is anyone who contributes to the database – this would include individual investigators, monitoring and compliance specialists, as well as support staff. The **administrator** role will be shared by system managers (for databases related to the program) and records managers (for systems of records created by systems managers and for records generated in carrying out the function). Finally **users** of the information will be ministry staff who have access to the system to carry out their work. Users may, in some cases, be employees of other ministries in the government, as well as industry associations or the business or organization under review.

Example #6: Electronic Information Management

As ministries implement electronic information management (EIM), a clear set of business rules need to be established about how the roles and responsibilities for managing content will be fulfilled. The business manager (or delegate) will be the **controller** of the information – defining the information needs and uses. The

steward of the information will be the individual who creates or collects the information. When the content item is placed in the EIM application, the steward will name the content and apply metadata to the content. The steward will also be responsible for making a decision about when the information should be declared an official record. Multiple individuals will fulfill the **administrator** role. These individuals include the Senior Records Officer (who manages the records retention and disposition requirements for the ministry), the local EIM administrator (who manages the use of the application within the business unit and works with other EIM administrators in establishing the business rules for using the EIM application), as well as the systems administrator (who manages the application for the ministry). Finally, the **user** will be anyone who has authorized access to the content item.

5.
Conclusion

Ministries will meet the accountability directive of the Information Management Framework in different ways. However, it is important to document and communicate what the accountability structure is for information management. As such, ministries will want to ensure their accountability structure includes:

- clear accountability statements for the management of information assets within the ministry;
- a mechanism for coordinating information management within the ministry and to ensure that information management is integrated with information and communications technology management; and
- clear identification and education around roles and responsibilities in specific business contexts.

It is critical that information assets be **managed** properly throughout their life-cycle, ensuring that necessary and appropriate information is collected or created, the information remains accurate, protected, and available for proper use, and that it is disposed of or preserved as required. By clearly establishing roles and responsibilities, ministries can be confident that their information assets are well managed and provide value to the users of the information (both internal and external to the ministry).